

REMARKS

Claims 1-53 are pending in the present application. Claims 3 and 7-8 have been amended to correct minor typographical errors.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 102(a)

Claims 1-53 were rejected under 35 U.S.C. §102(a) as being anticipated by Ekdahl et al., “SNOW – a new stream cipher”, Nov. 2001 (hereinafter referred to as the Ekdahl publication).

The rejection of claim 1 as being anticipated by the Ekdahl publication is respectfully traversed. Claim 1 recites, “A method of generating a key stream comprising: applying a cryptographic function on input values selected from a first array of values to generate output values; selecting mask values from a second array of values; and combining the output values with the mask values to generate a key stream block for the key stream; wherein the first and second arrays are finite.”. The Ekdahl publication fails to disclose a key stream block. Instead, the SNOW generator of the Ekdahl publication produces a running key (Fig. 1), by bitwise adding the output of the finite state machine (FSM) with the last entry (32 bits) of the LFSR. Further, as recited in claim 1, the input values, the output values, and the mask values, are plural, and the key stream block is singular. Exemplary input values are A, B, C, D and E selected from an array of values in LFSR 610, and exemplary mask values are A', B', C', D' and E' selected from a new or an updated array of values in LFSR 610 (Figure 6). The Ekdahl publication teaches combining only the last entry of the LFSR with the FSM output in a bitwise manner to generate the running key. Thus, only one 32-bit entry or value of the LFSR's array of values is selected and combined in generating the running key. Similarly, the 32-bit registers, R1 and R2, produce only one 32-bit value at a time. Also, the values of the registers R1 and R2 are not combined with last entry of the LFSR. Instead, the output of the FSM, which is not equal to either of the values of the registers, is combined with the last entry of the LFSR. Thus, the Ekdahl publication fails to disclose a key stream block, and fails to disclose combining the output values (plural) with the mask values (plural) to generate the key stream block. Thus, the Ekdahl publication fails to anticipate all of the features recited in claim 1. Accordingly, the rejection of claim 1 as being anticipated by the Ekdahl publication should be withdrawn.

It is respectfully submitted that dependent claims 2-26 are at least allowable for the reasons given above in relation to independent claim 1. Of particular note are claims 3-5 and 7, which associate the values of the first array with a LRSR. However, in the Office Action, with respect to claim 1, the Examiner associates the FSM with the first array of values, and then, with respect to claims 3-5, the Examiner associates the LFSR with the first array. See, Office Action, page 2, item 5, and page 4, item 8. Thus, the rejections of claims 2-5 and 7 are inconsistent with the rejection of claim 1. Also, claim 10 recites that “the first and second arrays each comprises seventeen values”. However, the FSM does not have seventeen registers, and the LFSR of the SNOW generator has only 16 registers.

Claims 27-53 are apparatus and computer readable medium claims having features defined by language similar to that of method claims 1-26. Claim 27 recites “means for combining the output values with the mask values to generate a key stream block for the key stream”, claim 37 recites, “combining the output values with the mask values to generate a key stream block for the key stream”, and claim 44 recites, “a combining module configured to combine the output values with mask values selected from a second array of values to generate a key stream block for the key stream”. Accordingly, for the reasons recited above with respect to claims 1-26, claims 27-53 define patentable advances over the Ekdahl publication, and the rejections of claims 27-53 should be withdrawn.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **December 21, 2007**

**By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295**

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502